Internet Engineering Task Force
Internet-Draft
Updates: RFC4253 (if approved)
Intended status: Standards Track
Expires: March 5, 2020

B. Harris

L. Velvindron
cyberstorm.mu

September 2, 2019

Ed25519 and Ed448 public key algorithms for the Secure Shell (SSH) protocol
draft-ietf-curdle-ssh-ed25519-ed448-10

Abstract

This document describes the use of the Ed25519 and Ed448 digital signature algorithm in the Secure Shell (SSH) protocol.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 5, 2020.

1. Introduction

Secure Shell (SSH) [RFC4251] is a secure remote-login protocol. It provides for an extensible variety of public key algorithms for identifying servers and users to one another. Ed25519 [RFC8032] is a digital signature system. OpenSSH 6.5 [OpenSSH-6.5] introduced support for using Ed25519 for server and user authentication and was then followed by other SSH implementations.

This document describes the method implemented by OpenSSH and others, and formalizes its use of the name "ssh-ed25519". Additionally, it also describes the use of Ed448 and formalizes its use of the name "ssh-ed448".

[TO BE REMOVED: Please send comments on this draft to curdle@ietf.org.]

2. Conventions Used in This Document

The descriptions of key and signature formats use the notation introduced in [RFC4251], Section 3 [RFC4251] and the string data type from [RFC4251], Section 5 [RFC4251].

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119] RFC 8174 [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Public Key Algorithm

This document describes a public key algorithm for use with SSH in accordance with [RFC4253], Section 6.6 [RFC4253]. The name of the algorithm is "ssh-ed25519". This algorithm only supports signing and not encryption.

Additionally, this document describes another public key algorithm. The name of the algorithm is "ssh-ed448". This algorithm only supports signing and not encryption.

Standard implementations of SSH SHOULD implement these signature algorithms.

4. Public Key Format

The "ssh-ed25519" key format has the following encoding:

```
string    "ssh-ed25519"
string    key
```

Here 'key' is the 32-octet public key described by [RFC8032], Section 5.1.5 [RFC8032].

The "ssh-ed448" key format has the following encoding:

```
string    "ssh-ed448"
string    key
```

Here 'key' is the 57-octet public key described by [RFC8032], Section 5.2.5 [RFC8032].

5. Signature Algorithm

Signatures are generated according to the procedure in [RFC8032], Section 5.1.6 and Section 5.2.6 [RFC8032].

6. Signature Format

The "ssh-ed25519" key format has the following encoding:

```
string    "ssh-ed25519"
string    signature
```

Here 'signature' is the 64-octet signature produced in accordance with [RFC8032], Section 5.1.6 [RFC8032].

The "ssh-ed448" key format has the following encoding:

```
string    "ssh-ed448"
string    signature
```

Here 'signature' is the 114-octet signature produced in accordance with [RFC8032], Section 5.2.6 [RFC8032].

7. Verification Algorithm

Ed25519 signatures are verified according to the procedure in [RFC8032], Section 5.1.7 [RFC8032].

Ed448 signatures are verified according to the procedure in [RFC8032], Section 5.2.7 [RFC8032].

8. SSHFP DNS resource records

Usage and generation of SSHFP DNS resource record is described in [RFC4255]. The generation of SSHFP resource records for "ssh-ed25519" keys is described in [RFC7479]. This section illustrates the generation of SSHFP resource records for "ssh-ed448" keys and the document specifies the corresponding Ed448 code point to the "SSHFP RR Types for public key algorithms" IANA registry.

The generation of SSHFP resource records for "ssh-ed25519" keys is described in [RFC7479].

The generation of SSHFP resource records for "ssh-ed448" keys is described as follows.

The encoding of ed448 public keys is described in [ED448]. In brief, an ed448 public key is a 57-octet value representing a 455-bit y-coordinate of an elliptic curve point, and a sign bit indicating the the corresponding x-coordinate.

The SSHFP Resource Record for the Ed448 public key with SHA-256 fingerprint would for example be:

example.com. IN SSHFP TBD 2 (a87f1b687ac0e57d2a081a2f2826723
34d90ed316d2b818ca9580ea384d924 01)

The 2 here indicates SHA-256 [RFC6594].

9. IANA Considerations

This document augments the Public Key Algorithm Names in [RFC4250], Section 4.6.2 [RFC4250].

IANA is requested to add to the Public Key Algorithm Names registry [IANA-PKA] with the following entry:

Public Key Algorithm Name	Reference
ssh-ed25519	This Draft
ssh-ed448	This Draft

IANA is requested to add the following entry to the "SSHFP RR Types for public key algorithms" registry [IANA-SSHFP]:

Value	Description	Reference

TBD	Ed448	[this-draft]

We strongly suggest 6 as value.

[TO BE REMOVED: This registration should take place at the following location: <http://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml#ssh-parameters-19>]

10. Security Considerations

The security considerations in [RFC4251], Section 9 [RFC4251] apply to all SSH implementations, including those using Ed25519 and Ed448.

The security considerations in [RFC8032], Section 8 [RFC8032] and [RFC7479] apply to all uses of Ed25519 and Ed448 including those in SSH.

11. Acknowledgements

The OpenSSH implementation of Ed25519 in SSH was written by Markus Friedl. We are also grateful to Mark Baushke, Benjamin Kaduk and Daniel Migault for their comments.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, DOI 10.17487/RFC4250, January 2006, <https://www.rfc-editor.org/info/rfc4250>.

[RFC4251] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, DOI 10.17487/RFC4251, January 2006, <https://www.rfc-editor.org/info/rfc4251>.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <https://www.rfc-editor.org/info/rfc4253>.

[RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC 4255, DOI 10.17487/RFC4255, January 2006, <https://www.rfc-editor.org/info/rfc4255>.

[RFC6594] Sury, O., "Use of the SHA-256 Algorithm with RSA, Digital Signature Algorithm (DSA), and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records", RFC 6594, DOI 10.17487/RFC6594, April 2012, <https://www.rfc-editor.org/info/rfc6594>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

12.2. Informative References

[ED448] Hamburg, M., "Ed448-Goldilocks, a new elliptic curve", January 2015, <https://eprint.iacr.org/2015/625.pdf>.

[IANA-PKA] Internet Assigned Numbers Authority (IANA), "Secure Shell (SSH) Protocol Parameters: Public Key Algorithm Names", May 2017, <http://www.iana.org/assignments/ssh-parameters/ssh-parameters.xhtml#ssh-parameters-19>.

[IANA-SSHFP] Internet Assigned Numbers Authority (IANA), "Secure Shell (SSH) Protocol Parameters: Public Key Algorithm Names", May 2017, <https://www.iana.org/assignments/dns-sshfp-rr-parameters/dns-sshfp-rr-parameters.xhtml#dns-sshfp-rr-parameters-1>.

[OpenSSH-6.5] Friedl, M., Provos, N., de Raadt, T., Steves, K., Miller, D., Tucker, D., Rice, T., and B. Lindstrom, "OpenSSH 6.5 release notes", January 2014, <http://www.openssh.com/txt/release-6.5>.

[RFC7479] Moonesamy, S., "Using Ed25519 in SSHFP Resource Records", RFC 7479, DOI 10.17487/RFC7479, March 2015, <https://www.rfc-editor.org/info/rfc7479>.

Authors' Addresses

Ben Harris
2A Eachard Road
CAMBRIDGE CB3 0HY
UNITED KINGDOM

Email: bjh21@bjh21.me.uk

Loganaden Velvindron
cyberstorm.mu
88, Avenue De Plevitz
Roches Brunes
Mauritius

Email: logan@cyberstorm.mu